UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
14/494,844	09/24/2014	Yong Zhang	FORT-014200	7193

64128 7590 04/24/2017

MICHAEL A DESANCTIS
HAMILTON DESANCTIS & CHA LLP
FINANCIAL PLAZA AT UNION SQUARE
225 UNION BOULEVARD, SUITE 150
LAKEWOOD, CO 80228

EXAMINER	
KORSAK, OLEG	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
04/24/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

mdesanctis@hdciplaw.com
docket@hdciplaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte YONG ZHANG[1]

Appeal 2017-003231
Application 14/494,844
Technology Center 2400

Before JOHNNY A. KUMAR, TERRENCE W. McMILLIN, and SCOTT E. BAIN, *Administrative Patent Judges*.

KUMAR, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1–17. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

---

[1] Appellant identifies Fortinet, Inc. as the real party in interest (Br. 3).

STATEMENT OF THE CASE

Exemplary claim 1 recites:

1. A method comprising:

receiving, by a wireless network controller of a wireless local area network (WLAN), an authentication request relating to a wireless client device from a wireless access point (AP) managed by the wireless network controller;

determining, by the wireless network controller, whether a prior authentication result associated with the wireless client device is present in a cache of the wireless network controller;

permitting, by the wireless network controller, the wireless client device to access the WLAN via the AP when the prior authentication result is present and indicates the wireless client device was successfully authenticated;

issuing, by the wireless network controller, the authentication request to a remote authentication device associated with the WLAN to determine a current authentication status of the wireless client device;

receiving, by the wireless network controller, the current authentication status of the wireless client device from the remote authentication device;

storing, by the wireless network controller, information regarding the current authentication status within the cache.

Rejections

Claims 1–3 and 5–17 are rejected under 35 U.S.C. § 102(a)(1) as being anticipated by Zhang (Haojun Zhang & Yuefei Zhu, *A New Authentication And Key Management Scheme of WLAN*, IEEE (2006)). Final Act. 2–5.

Claim 4 is rejected under 35 U.S.C. § 103 as being unpatentable over Zhang and Morris (US 2007/0209081 A1, Sept. 6, 2007). Final Act. 6–7.

ANALYSIS

Rather than reiterate the arguments of Appellant and the Examiner, we refer to the Final Office Action ("Final Act.") mailed April 20, 2015, the Appeal Brief ("Br.") filed February 8, 2016, and the Examiner's Answer ("Ans.") mailed July 28, 2016, for the respective details. We have considered in this decision only those arguments Appellant actually raised in the Briefs. Any other arguments that Appellant could have made, but chose not to make in the Briefs are deemed to be waived. *See* 37 C.F.R. § 41.37(c)(1)(vii).

On pages 2 through 8 of the Final Office Action and pages 2 through 7 of the Answer, the Examiner has provided a comprehensive response to each argument presented by the Appellant. We have reviewed this response and concur with the Examiner's findings and conclusions. We adopt as our own the findings and reasons set forth by the Examiner in the Final Office Action (Final Act. 2–7) and the Examiner's Answer in response to Appellant's Appeal Brief (Ans. 2–7). We highlight and address specific findings and arguments for emphasis as follows.

Section 102 rejection of claims 1-3, and 5-17 over Zhang

Based on Appellant's arguments in the Appeal Brief (Br. 12–15), the dispositive issues regarding whether the Examiner erred in rejecting claims 1–3 and 5–17 are whether Zhang discloses the following limitations in claim 1 (emphasis added): [2]

> [a] determining, by the *wireless network controller*, whether a prior authentication result associated with the

[2] Independent claim 10 recites subject matter similar to independent claim 1. Br. 14–15.

> wireless client device is present in a cache of the wireless network controller;
>
> [b] permitting, by the wireless network controller, the wireless client device to access the WLAN via the AP *when the prior authentication result is present and indicates the wireless client device was successfully authenticated*[.]
>
> Regarding disputed limitation [a], Appellant contends:
>
> [T]he wireless network controller and the AS are *distinct and separate* elements. See, e.g., Specification at FIG. 1 (in which both a wireless network controller and various types of authentication servers, e.g., LDAP server 108-1, remote server 108-2 and RADIUS server 108-3, are separately depicted) and ¶ [0047]. As noted above, in the context of Zhang, all authentication requests (i.e., protocol flow or conversation message S2 are directed to and serviced by the AS). As also noted above, the caching described by Zhang is performed by the AS. No caching is taught or reasonably suggested by Zhang to be performed by a wireless network controller as required by independent claim 1.

Br. 14 (emphasis in original omitted, emphasis added).

In response, the Examiner finds, and we agree, Zhang discloses the claimed "wireless network controller":

> In summary the main and only Appellant's argument is that all functionality (receiving, determining, permitting) disclosed by Zhang and relevant to limitations of claims 1-3 and 5-17 applies to AS of Zhang, which is different from claimed wireless network controller, because it is *separate* from AP as shown at FIG. 1 of Specification. However, *Examiner puts on record that no physically separate feature is currently claimed*, and the only limitation is that AP managed by the wireless network controller (see receiving step of Claim 1 and a client request receive module of Claim 10). Zhang teaches that caching and other functionalities can be physically embedded with AP: "As a good choice, APs can cache STAs' TVPKs transmitted from the AS. Certainly this needs some schemes to

> ensure all TVPKs cached in APs are coherent and are updated synchronously. There are many methods or strategies satisfying this need. In this case, messages are first filtered by the AP before being delivered to the AS" (Zhang, pages 4-5), which is essentially what is claimed in claim 1. And even motivations by Zhang and Appellant are the same. Compare Overview, (Appeal Brief, page 7) with "Another significant feature of our scheme is that authenticating STAs is efficient and can be accomplished in the first protocol flow, that is, in the foremost time. Another highlight of the proposed scheme is that it is possible to authenticate STAs in the AP (caching TVPKs) to prevent illegal message from transferring to the AS" (Zhang, page 4).

Ans. 3.

In other words, in Zhang "the AS can verify it efficiently by computing $h(Token^{i}_{STA})$ and compares it with the previous token $Token^{i-1}_{STA}$ cached in the AS." *Id.* at 4 (citing Zhang, 3.2 (The Basic Scheme)). The Examiner notes, "Zhang teaches that it is possible to authenticate STAs in the AP (caching TVPKs)." *Id.* (citing Zhang, page 4).

In addition, Appellant's arguments are not commensurate with the scope of the claims because claim 1 does not preclude the wireless network controller and the AS from being *distinct and separate* elements.

> Regarding disputed limitation [b], the Examiner finds, and we agree
>
> Applicant relies in his arguments on S2 Auth Request shown in Zhang at Figure 3. Authentication & Pair-Keys Negotiation in FWAI. Describing Figure 3 Zhang teaches: "A STA logs in WLAN in i-th time with the token $Token^{i}STA=h^{N-I}(S)$, and the AS can verify it efficiently by computing $h(Token^{i}STA)$ and compares it with the previous token $Token^{i-1}STA$ cached in the AS. If the token is valid, *the AS authenticates the STA* successfully and records this token as the TVPK for the STA." (Zhang, page 3) (emphasis added).

> Examiner considers "*information regarding the current authentication status" of Applicant to be equivalent the TVPK token of Zhang*, Further *cached information of Applicant is the same as* $TVPK^{i-1}$*, and the current is the same as* $TVPK^{i}$.
>
> And finally, contrary to Applicant assertion that Zhang requires an authentication request (i.e., protocol flow or conversation message S2) to be issued to and serviced by the AS before the STA is provided access to the WLAN, Zhang strongly teaches that: "*Another highlight of the proposed scheme is that it is possible to authenticate STAs in the AP (caching TVPKs) to prevent illegal message from transferring to the AS.*"

Ans. 5 (emphasis added).

Thus, Appellant has not shown error in the Examiner's rejection of claims 1–3 and 5–17. Appellant has not further responded to these explanations, because no Reply Brief was filed.

Section 103 rejection of claim 4 over Zhang and Morris

Appellant provided additional arguments with respect to the patentability of claim 4 (Br. 15–16). We have considered these arguments and find them unpersuasive. In addition, we note the Examiner has rebutted these arguments in the Answer by a preponderance of the evidence (Ans. 6). We agree with the Examiner's findings and underlying reasoning and adopt them as our own. Consequently, we conclude there is no reversible error in the Examiner's rejections of claim 4.

DECISION

The Examiner's rejections of claims 1–17 are affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED